Uma imagem com texto

Descrição gerada automaticamente

TeSP de CiberSegurança e Redes Informática

Lourenço Eduardo Estêvão Pereira Índio – 2231606

Diogo

Antonio

Trabalho da Unidade Curricular de SRS

Leiria, novembro de 2024

# Lista de Imagens

[Imagem 1 - Configurações da Máquina Virtual 5](#_Toc162194076)

[Imagem 2 - Máquina Virtual criada 5](#_Toc162194077)

[Imagem 4 - Árvore 7](#_Toc162194078)

[Imagem 5 - Passo 1 da instalação Domínio 8](#_Toc162194079)

[Imagem 6 - Passo 2 da instalação Domínio 8](#_Toc162194080)

[Imagem 7 - Instalação Finalizada 9](#_Toc162194081)

[Imagem 8 - Computadores criados 9](#_Toc162194082)

[Imagem 9 - Utilizadores criados 9](#_Toc162194083)

[Imagem 10 - Grupos criados 10](#_Toc162194084)

[Imagem 11 - Script usado 10](#_Toc162194085)

[Imagem 12 . Delegar Tarefas de Gestão 11](#_Toc162194086)

[Imagem 13 - Permissões 11](#_Toc162194087)

[Imagem 14 - Definição da Hora 12](#_Toc162194088)

# Lista de siglas e acrónimos

|  |  |
| --- | --- |
| ESTG | Escola Superior de Tecnologia e Gestão |
| IPLeiria | Instituto Politécnico de Leiria |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Índice

[Lista de Figuras ii](#_Toc161304882)

[Lista de tabelas iv](#_Toc161304883)

[Lista de siglas e acrónimos v](#_Toc161304884)

[1. Introdução 1](#_Toc161304885)

[1.1. O objeto do trabalho 1](#_Toc161304886)

[1.2. Definição de sistema informático 1](#_Toc161304887)

[1.3. Apresentação das funções e da administração de sistemas 1](#_Toc161304888)

[1.4. Apresentação das funções e da gestão de sistemas 1](#_Toc161304889)

[1.5. Apresentação da empresa 2](#_Toc161304890)

[1.6. Estrutura do documento 3](#_Toc161304891)

[2. Virtualização e Sistema Operativo 4](#_Toc161304892)

[2.1. Máquinas Virtuais 4](#_Toc161304893)

[2.2. VirtualBox, VMWare e Hyper-V 4](#_Toc161304894)

[2.3. Criação da máquina virtual 5](#_Toc161304895)

[2.4. Sistemas operativos servidores 6](#_Toc161304896)

[2.5. Instalação dos sistemas operativo 6](#_Toc161304897)

[3. Criação do domínio 7](#_Toc161304898)

[3.1. Definição de conceitos 7](#_Toc161304899)

[3.1.1. Domínio, árvore e floresta de domínios 7](#_Toc161304900)

[3.1.2. Controlador de domínio 8](#_Toc161304901)

[3.1.3. Active Directory 8](#_Toc161304902)

[3.2. Instalação e criação do domínio 8](#_Toc161304903)

[4. Configuração e manutenção da Active Directory 9](#_Toc161304904)

[4.1. Definição de regras utilizadas na configuração da AD 9](#_Toc161304905)

[4.2. Configuração da AD 9](#_Toc161304906)

[4.3. Criação de processos automáticos para a configuração da AD 9](#_Toc161304907)

[4.4. Configuração de elementos específicos da AD Erro! Marcador não definido.](#_Toc161304908)

[4.4.1. Regras sobre a manutenção e utilização da conta Administrador 10](#_Toc161304909)

[4.4.2. Regras sobre a manutenção e utilização da conta Convidado 10](#_Toc161304910)

[4.4.3. Delegação de tarefas de Gestão 11](#_Toc161304911)

[4.4.4. Criação de contas de serviços e permissões 11](#_Toc161304912)

[4.5. Configuração e gestão de tarefas de registo de eventos, monitorização e auditoria. 12](#_Toc161304913)

[4.5.1. Registo de eventos 12](#_Toc161304914)

[4.5.2. Monitorização e auditoria 12](#_Toc161304915)

[4.5.3. Definição da hora 12](#_Toc161304916)

[5. Conclusões 13](#_Toc161304917)

[6. Bibliografia 14](#_Toc161304918)

# Introdução

Neste relatório, apresenta-se a fase inicial do desenvolvimento de uma rede e serviços para uma empresa Este projeto visa estabelecer um ambiente seguro e eficiente, correspondendo às necessidades de uma empresa que lida com clientes, serviços, rede e servidores.

## Objetivo do trabalho

Este trabalho será realizado no âmbito da UC de SRS do curso CRI e tem por objetivo, desenvolver uma infraestrutura de rede e serviços segura e eficiente para a empresa uma determinada empresa. Deve permitir que a empresa ofereça suas soluções e plataformas com confiabilidade e segurança.

Serão configurados e implementados serviços essenciais que achamos essenciais como: Serviços de rede e conectividade para garantir uma comunicação segure entre utilizadores, serviços de acesso remoto para facilitar a gestão de maneira mais segura.

# Caso de Estudo

## Serviço de Email

O serviço de email é essencial para a comunicação interna e externa de qualquer empresa, permite que os colaboradores enviem e recebam emails de forma segura, seja para comunicação interna ou para contato com clientes externos.

Contas:

## Serviço de Monitorização

O serviço de monitorização é crucial para garantir a operação contínua e eficiente dos sistemas e serviços da empresa, permite que a equipe de TI acompanhe o desempenho, a disponibilidade e a integridade dos recursos de rede, detetando e respondendo rapidamente a possíveis problemas ou falhas que poderão acontecer.

Para implementar este serviço, iremos utilizar o NAGIOS, é um serviço popular e confiável para monitorizar a rede e servidores. O NAGIOS permite monitorizar vários aspetos dos sistemas bem como: disponibilidade de serviços, desempenho de recurso e até mesmo enviar alertas de possíveis problemas.

## Serviço de Acesso Remoto

O serviço de acesso remoto permite que os administradores gerenciem os servidores de forma segura, podendo os mesmos estar fora das instalações da empresa. Esse acesso é fundamental para realizar tarefas de manutenção, atualização e resposta a incidentes de forma rápida e eficiente.

O OpenSSH é um software de acesso remoto, devido à sua segurança e flexibilidade ele é amplamente utilizado para conexões seguras, permitindo o acesso a servidores via protocolo SSH (Secure Shell).

**Configurações de Segurança**:

* **Autenticação por Chave SSH**: A autenticação será feita através da chave SSH, que são mais seguras. Somente usuários com a chave privada irão conseguir ter acesso aos servidores.
* **Criptografia RSA**: Será utilizada a criptografia RSA para a geração das chaves, garantindo assim um nível de alta segurança.
* **Tamanho da Chave**: A chave será gerada com um tamanho de 4096 bits
* **Armazenamento da Chave Privada**: A chave privada será armazenada com segurança pelos administradores da rede, em dispositivos seguros e protegidos por senha, para evitar que seja acedida por terceiros.

**Quem vai utilizar?**

O acesso remoto será distribuído aos administradores do sistema responsáveis pela manutenção e monitorização dos servidores. Cada utilizador autorizado terá sua própria chave SSH, permitindo auditoria e controle de acesso.

# Serviços de Rede Seguros

## Serviço de nomes (DNS)

O serviço de nomes ou DNS (Domain Name System), é responsável pela resolução de nomes de domínio em endereços IP, permitindo que os utilizadores acesse aos serviços e sites da empresa por meio de nomes em vez de endereços IP numéricos. Esse serviço é essencial para a navegação e comunicação em rede, tanto para acesso interno quanto externo.

O BIND (Berkeley Internet Name Domain) é um software de DNS, pois é um dos mais populares e confiáveis para implementação de serviços DNS, com suporte para as principais funcionalidades de segurança e redundância.

### Domínio, árvore e floresta de domínios



Imagem 5 - Dominio

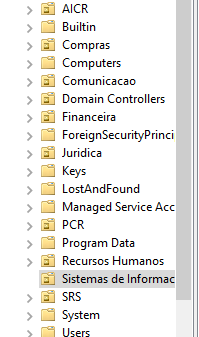


Imagem 6 - Árvore

### Controlador de domínio

Um controlador de domínio é um componente essencial em um ambiente baseado no Windows Server e no Active Directory. A função que desempenha é armazenar e gerenciar informações de segurança e políticas para um domínio específico. Funções como: autenticação de utilizadores, autorização de acesso, implementação de políticas de grupo entre outras.

### Active Directory

O Active Directory funciona como um serviço de diretório, que é uma base de dados hierárquica que armazena informações sobre os recursos de rede da empresa, também permite a criação e aplicação de políticas de grupo, que são conjuntos de configurações que podem ser aplicadas a utilizadores e computadores para controlar seu ambiente de trabalho

## Instalação e criação do domínio

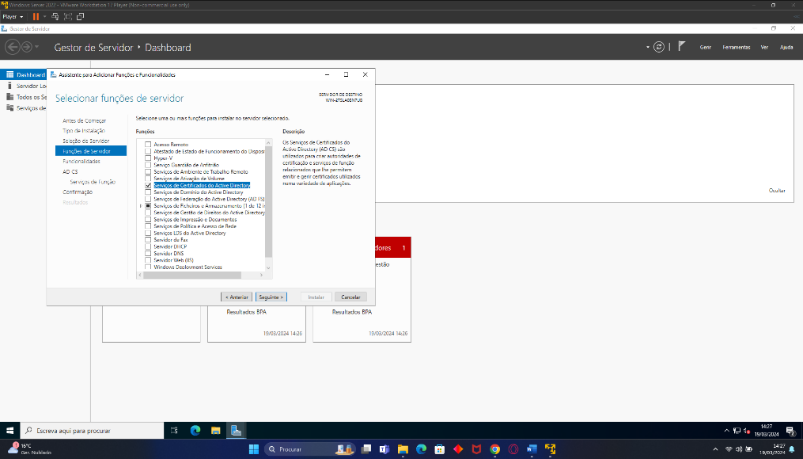


Imagem 7 - Passo 1 da instalação Domínio

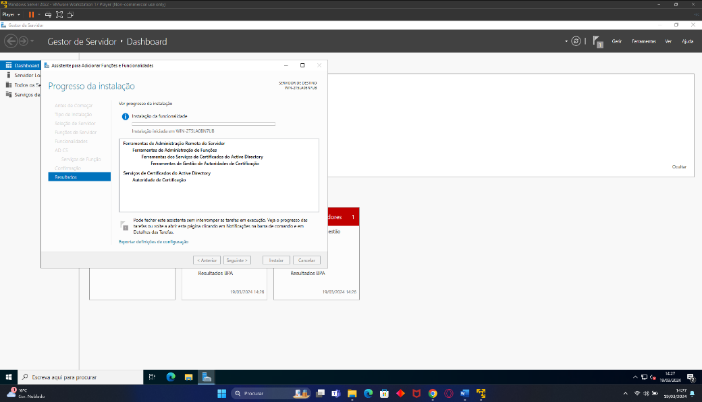


Imagem 8 - Passo 2 da instalação Domínio

# Configuração e manutenção da Active Directory

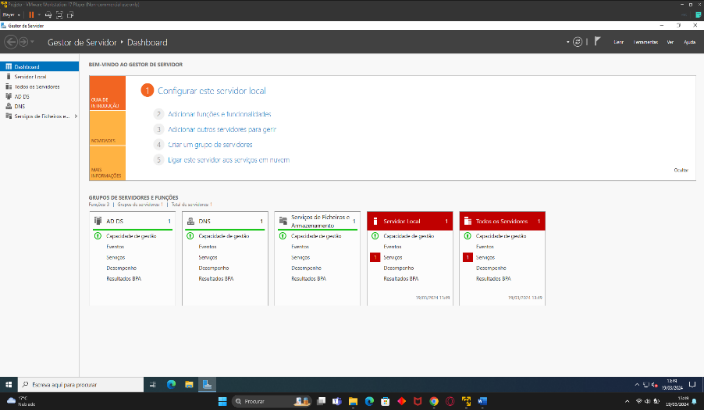


Imagem 9 - Instalação Finalizada

## Definição de regras utilizadas na configuração da AD

Separar as contas de user das de computadores, criar uma OU específica para grupos de segurança, usar uma convenção de nomes padronizada.

## Configuração da AD

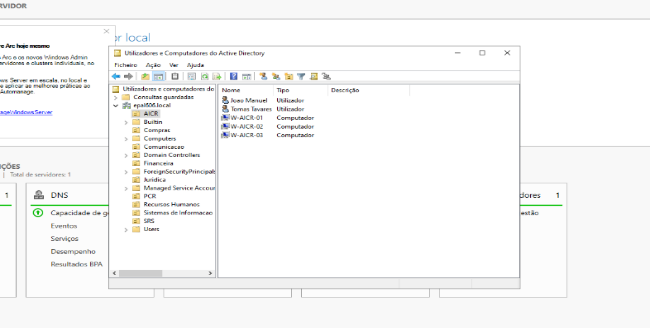


Imagem 10 - Computadores criados

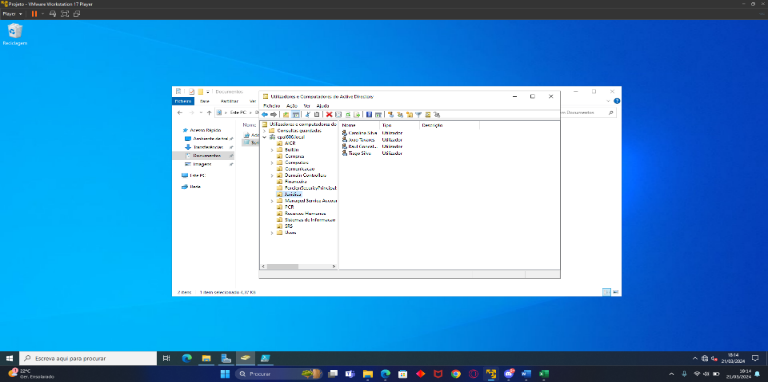


Imagem 11 - Utilizadores criados

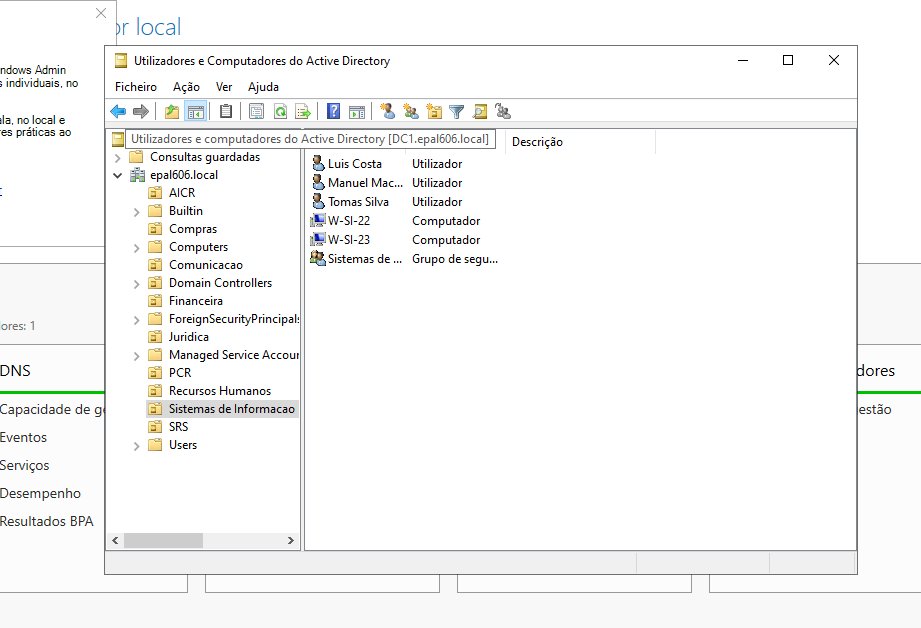


Imagem 12 - Grupos criados

## Criação de processos automáticos para a configuração da AD

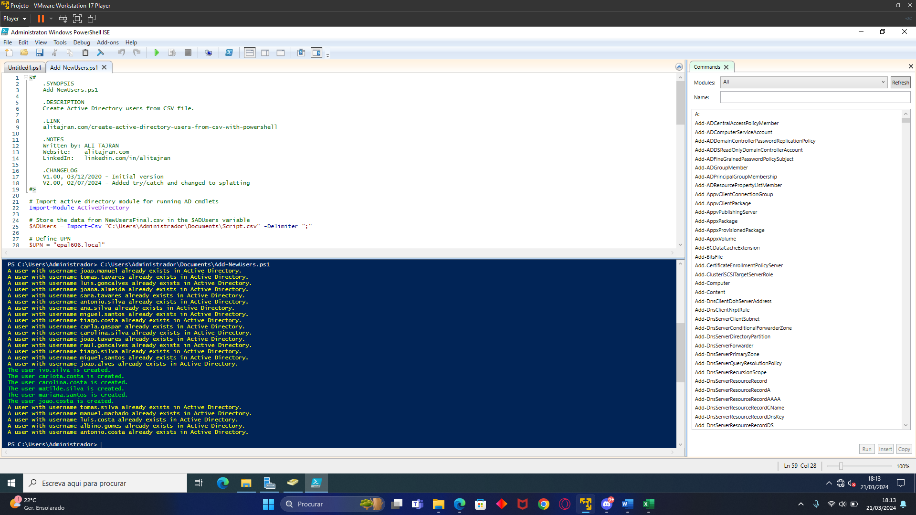


Imagem 13 - Script usado

### Regras sobre a manutenção e utilização da conta Administrador

A conta de Administrador deve ser utilizada apenas para tarefas que exijam privilégios elevados.

### Regras sobre a manutenção e utilização da conta Convidado

A conta Convidado deve ser utilizada apenas para acesso temporário e limitado a recursos públicos ou compartilhados que não exijam autenticação de utilizador. Restringir o acesso da conta Convidado apenas aos recursos necessários.

### Delegação de tarefas de Gestão

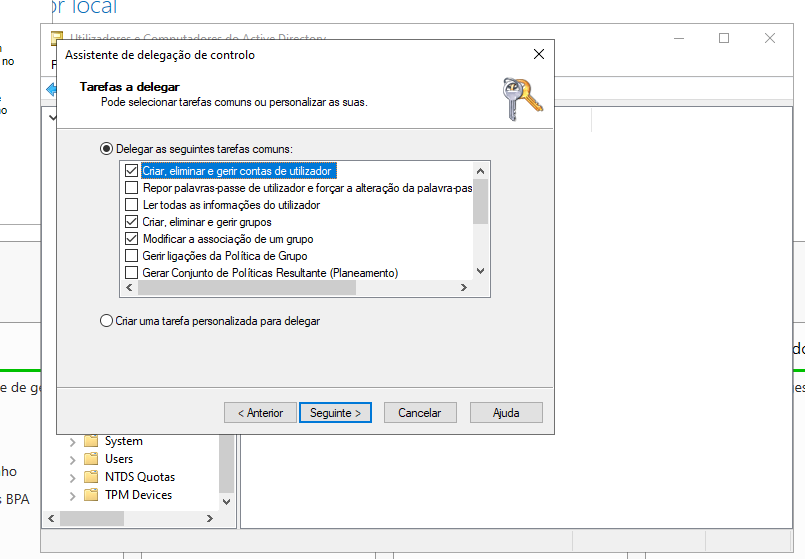


Imagem 14 - Delegar Tarefas de Gestão

### Criação de contas de serviços e permissões

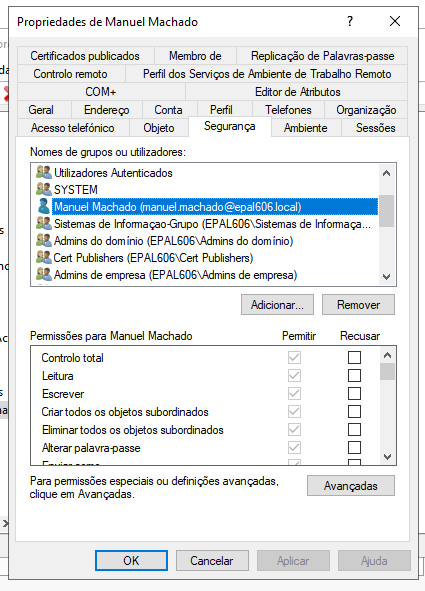


Imagem 15 - Permissões

## Configuração e gestão de tarefas de registo de eventos, monitorização e auditoria.

A configuração e gestão de registos de eventos, monitoramento contínuo e auditorias regulares são importantes para a segurança e integridade dos sistemas de informação. A definição de eventos a serem registados, a deteção de anomalias protege os dados e assegura a continuidade de um bom serviço.

### Registo de eventos

O registo de eventos é uma funcionalidade que captura e armazena informações sobre eventos e atividades que ocorrem em um sistema, como por exemplos erros, alertas, informações de segurança, alterações de configuração entre outras.

### Monitorização e auditoria

A monitorização e a auditoria são práticas essenciais para garantir a segurança, desempenho e conformidade de um ambiente de tecnologia da informação. Elas envolvem o acompanhamento contínuo das atividades, eventos e métricas de sistemas.

### Definição da hora

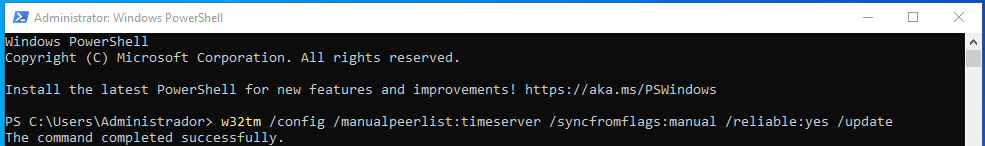


Imagem 16 - Definição da Hora

# Conclusões

Concluir esta etapa foi importante para compreender os conceitos básicos do Windows Server, algumas configurações a implementar. Na minha opinião é importante saber primeiros estes conceitos para depois passar para a prática, e assim fica muito mais fácil saber o que estamos a fazer. Existem algumas funcionalidades e regras que não foram implementadas como por exemplo separar os Users dos Computadores que serão implementadas na segunda etapa. A maior dificuldade sentida foi na delegação de tarefas.

# Bibliografia

<https://www.alitajran.com/create-active-directory-users-from-csv-with-powershell/>

<https://www.linkedin.com/pulse/explorando-os-fundamentos-e-aplica%C3%A7%C3%B5es-da-anderson-vieira-machado-1nxuf/?originalSubdomain=pt>

<https://www.linkedin.com/pulse/boas-pr%C3%A1ticas-de-seguran%C3%A7a-para-m%C3%A1quinas-virtuais-em-nuvem-ag%C3%A1pto/?originalSubdomain=pt>

<https://pt.wikipedia.org/wiki/VirtualBox>

<https://www.vmware.com/pdf/ws_specs_pt.pdf>